MEDICAL IMAGE WATERMARKING SCHEME USING 13 BITS ENHANCED BLOCK AVEARGE INTENSITY

TAN GUI JIU

THESIS SUBMITTED IN FULFILMENT OF THE DEGREE OF COMPUTER SCIENCE

FACULTY OF COMPUTER SYSTEM AND SOFTWARE ENGINEERING

2013

ABSTRACT

This research is proposed the watermarking scheme in tamper localization which is able to detect the location of the manipulated areas and verify the authentic by using the block average intensity. The watermark data for ROI will store in the region of RONI. The embedded watermark allows the image have been tamper can recover and check for the tampering detection. The usage of the block average intensity is one of the popular techniques due to its easy to implementation. In this research, the tamper localization will performed using block average intensity in the tamper watermarking scheme for medical image. The block average intensity and the sub-block average intensity will be used to find out the tamper area by using the authentication bit, parity check bit and average authentication bit.

ABSTRAK

Kajian ini mencadangkan tanda air dalam penyetempatan tamper yang mampu mengesan lokasi kawasan dimanipulasi dan mengesahkan yang sahih dengan menggunakan keamatan purata blok. Data tanda air untuk ROI akan menyimpan di rantau ini RONI. The watermark tertanam membolehkan imej yang telah mengganggu boleh pulih dan memeriksa pengesanan mengganggu. Penggunaan keamatan purata blok adalah salah satu teknik yang popular kerana yang mudah untuk dilaksanakan. Dalam kajian ini, localization tamper akan prestasi yang menggunakan keamatan purata blok dalam skim bega tanda air untuk imej perubatan. Keamatan purata blok dan keamatan purata sub-blok akan digunakan untuk mengetahui kawasan tamper dengan menggunakan sedikit pengesahan, persamaan memeriksa sedikit dan sedikit pengesahan purata.

TABLE OF CONTENTS

STUDENT'S DECLARATION		**iv**
SUPERVISOR'S DECLARATION		**v**
ACKNOWLEDGEMENTS		**vi**
ABSTRACT		**vii**
ABTRAK		**viii**
TABLE OF CONTENTS		**ix**
LIST OF TABLES		**xii**
LIST OF FIGURES		**xii**
LIST OF ABBREVIATIONS		**xvii**

SECTION	**CONTENT**	**PAGE**
1	**INTRODUCTION**	
1.1	Introduction	1
1.2	Problem Statement	3
1.3	Objective	3
1.4	Scope of Project	4
1.5	Thesis Organization	4
2	**LITERATURE REVIEW**	
2.1	Introduction	6
2.2	Type of Domain	6
2.2.1	Spatial Domain	6

2.2.2	Frequency Domain	7
2.3	Reversible Watermark	7
2.4	Region of Interest	7
2.5	Medical Image Watermarking	8
2.6	Tamper Localization	9
2.6.1	Overview of Watermarking Techniques	9
2.6.2	Other Examples of Schemes	11
3	**METHODOLOGY**	
3.1	Introduction	14
3.2	Methodology	14
3.3	Tampered Localization and Recovery	16
3.3.1	Authentication and Recovery Watermark	21
3.3.2	Watermark Generation and Embedding	22
3.3.2.1	Authentication and Recovery Watermark	22
3.3.3	Tamper Localization and Recovery	25
3.4	Expected Result	29
3.5	Hardware and Software Use	30
3.5.1	Hardware	30
3.5.2	Software	31
3.6	Conclusion	31
4	**RESULT AND DISCUSSION**	
4.1	Introduction	32
4.2	Overview	32
4.3	Solution by Using Enhanced Block Average Intensity	33
4.4	Watermark Ultrasound Image	37
4.5	Outcome of Ultrasound Image	42
4.5.1	Tamper Detected by Using 9 bits	42
4.5.2	Tamper Detected by Using 13 bits	54

4.6	Result	66
4.7	Conclusion	69
5	**CONCLUSION AND FUTURE WORK**	
5.1	Introduction	70
5.2	Contribution and Limitations	70
5.3	Future Work	71
5.4	Conclusion	71
	REFERENCES	72
	APPENDIX A	
	Coding	78
	APPENDIX B	
	Project Gannt Chart	108

LIST OF TABLES

TABLE NUMBER	TITLE	PAGE
Table 3.1	Purpose of each hardware use	27
Table 3.2	Purpose of each hardware use	28
Table 4.1	Comparison success rate by using noise	66
Table 4.2	Comparison success rate by using comparison of sharpen and noise	66
Table 4.3	Comparison success rate by using comparison of salt and noise	67
Table 4.4	Comparison success rate by using comparison of blur and noise	67
Table 4.5	Type of tamper for each sample	68

LIST OF FIGURES

FIGURE NUMBER	TITLE	PAGE
Figure 1	The authentication and parity check for the original block and tampered block	2
Figure 3.1	Sample 1 ultrasound image that have divided into ROI and RONI	17
Figure 3.2	Sample 2 ultrasound image that have divided into ROI and RONI	18
Figure 3.3	Sample 3 ultrasound image that have divided into ROI and RONI	19
Figure 3.4	Sample 4 ultrasound image that have divided into ROI and RONI	20
Figure 3.5	A block is divided into for sub-blocks	21
Figure 3.6	The block of 3 X 3 pixels where it contains one parity bit, one authentication bit and 7 recovery bit transformation	23
Figure 3.7	The authentication bit, v, and parity check bit, p, for the block	25
Figure 3.8	The authentication bit, v', and parity check bit, p', for the tampered block	26
Figure 3.9	Solution of the average authentication bit, A, will be used to solve the problem	28
Figure 3.10	The authentication bit, v, parity check bit, p, and average authentication bit, A, for a block	29

Figure 3.11	The authentication bit, v', parity check bit, p', and average authentication bit, A', for a tampered block	29
Figure 4.1	The 8 X 8 pixels block is further divided into 4 X 4 sub-block	34
Figure 4.2	Sample 1 ultrasound image with size 640 X 480 pixels	35
Figure 4.3	Sample 2 ultrasound image with size 640 X 480 pixels	36
Figure 4.4	Sample 3 ultrasound image with size 640 X 480 pixels	36
Figure 4.5	Sample 4 ultrasound image with size 640 X 480 pixels	37
Figure 4.6	Sample 1 image original ultrasound image	38
Figure 4.7	Sample 1 watermark Image	38
Figure 4.8	Sample 2 image original ultrasound image	39
Figure 4.9	Sample 2 watermark Image	39
Figure 4.10	Sample 3 image original ultrasound image	40
Figure 4.11	Sample 3 watermark Image	40
Figure 4.12	Sample 4 image original ultrasound image	41
Figure 4.13	Sample 4 watermark Image	41
Figure 4.14	Sample 1 with 9 bits tampered image using noise	43
Figure 4.15	Sample 1 with 9 bits tampered image using combination of sharpen and noise	43
Figure 4.16	Sample 1 with 9 bits tampered image using combination of salt and noise	44
Figure 4.17	Sample 1 with 9 bits tampered image using combination of blur and noise	44
Figure 4.18	Sample 2 with 9 bits tampered image using noise	45
Figure 4.19	Sample 2 with 9 bits tampered image using combination of sharpen and noise	46
Figure 4.20	Sample 2 with 9 bits tampered image using combination of salt and noise	46
Figure 4.21	Sample 2 with 9 bits tampered image using combination of blur and noise	47

Figure 4.22	Sample 3 with 9 bits tampered image using noise	48
Figure 4.23	Sample 3 with 9 bits tampered image using combination of sharpen and noise	49
Figure 4.24	Sample 3 with 9 bits tampered image using combination of salt and noise	49
Figure 4.25	Sample 3 with 9 bits tampered image using combination of blur and noise	50
Figure 4.26	Sample 4 with 9 bits tampered image using noise	51
Figure 4.27	Sample 4 with 9 bits tampered image using combination of sharpen and noise	52
Figure 4.28	Sample 4 with 9 bits tampered image using combination of salt and noise	52
Figure 4.29	Sample 4 with 9 bits tampered image using combination of blur and noise	53
Figure 4.30	Sample 1 with 13 bits tampered image using noise	54
Figure 4.31	Sample 1 with 13 bits tampered image using combination of sharpen and noise	55
Figure 4.32	Sample 1 with 13 bits tampered image using combination of salt and noise	55
Figure 4.33	Sample 1 with 13 bits tampered image using combination of blur and noise	56
Figure 4.34	Sample 2 with 13 bits tampered image using noise	57
Figure 4.35	Sample 2 with 13 bits tampered image using combination of sharpen and noise	58
Figure 4.36	Sample 2 with 13 bits tampered image using combination of salt and noise	58
Figure 4.37	Sample 2 with 13 bits tampered image using combination of blur and noise	59
Figure 4.38	Sample 3 with 13 bits tampered image using noise	60

Figure 4.39	Sample 3 with 13 bits tampered image using combination of sharpen and noise	61
Figure 4.40	Sample 3 with 13 bits tampered image using combination of salt and noise	61
Figure 4.41	Sample 3 with 13 bits tampered image using combination of blur and noise	62
Figure 4.42	Sample 4 with 13 bits tampered image using noise	63
Figure 4.43	Sample 4 with 13 bits tampered image using combination of sharpen and noise	64
Figure 4.44	Sample 4 with 13 bits tampered image using combination of salt and noise	64
Figure 4.45	Sample 4 with 13 bits tampered image using combination of blur and noise	65

LIST OF ABBREVIATIONS

ROI : Region of interest

RONI : Region of non-interest

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

Since in this era science and technology, there are a lot of illegal medical image claims. Watermarking can be used in medical field to prevent unlicensed modification by authenticating the content of image. Tamper localization can able watermarking scheme to detect and locate the modification of pixel values on the image. The tampered area can be recovered by recapture the original pixel values that were stored in the image itself as a watermark.

By using block average intensity the information can be reclaimed once the tampering was detected. So, if a block is being tampered locally, the pixel intensities will be changed and directly changes the average intensity of the concern block. In order to overcome these issues, a parity check is used. But, by using the parity check it also has disadvantages whereby if more than one bit is changed, the parity check is ineffective.

Besides that, the local tampering will cause an error when the same location was tampered with different pixels value. This is because when it has more than one parity has been changed a parity check is not longer to be useful. However, to ensure the better security, an additional feature is used by comparing the average intensity of a block with its sub-blocks.

Figure 1 below shows the authentication and parity check for the original block and tampered block. Based on the figure below, the average intensity of the block is 85. However, the average intensity of the sub-blocks is 99, 84, 81 and 77. The value of v represent the authentication bit of each block and p represent the parity check of each block were computed based on the average intensities and embedded as a part of the watermark. The two sub-blocks that locate at the first row were tampered and where the average intensities had been changed to 101 and 82 respectively. After the block had been tampered the average for the block is still remain unchanged and the value is still 85.

So, during the tamper detection process, the authentication bit and parity check bit is computed and denoted as v' and p'. However, the values of v' and p' for the sub-blocks in the first row is also remain unchanged. In this situation, the tampered sub-block will pass the detection process and left unrecovered when the embedded v and p were retrieved for comparison.

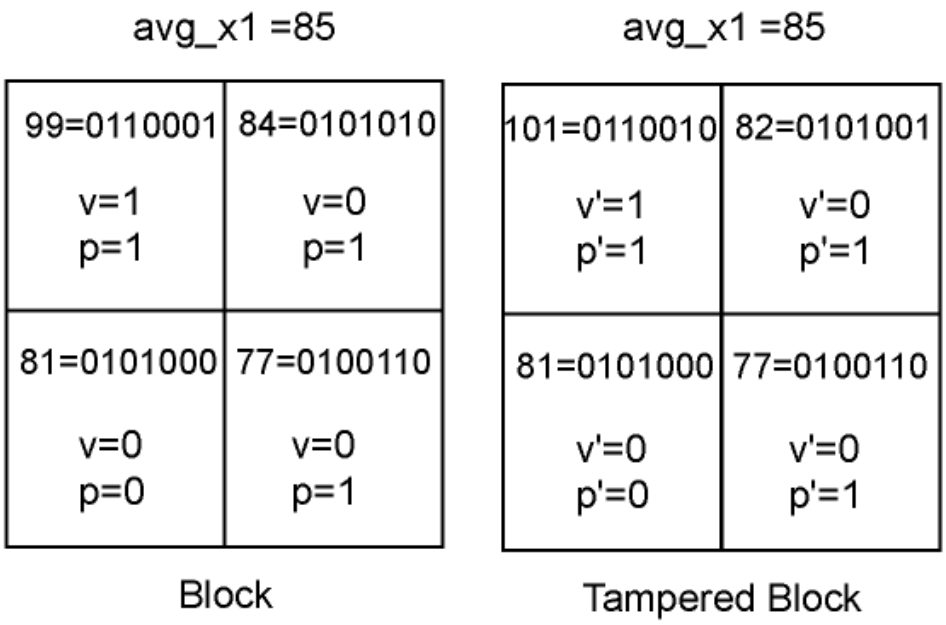

Figure 1: The authentication and parity check bit for the original block and tampered block.

As a conclusion, the usage of block average intensity in tamper localization is easy to perform without much computation is needed. It can use for recovery purposes. However based on tamper localization technique by using the block average intensity will fail in certain condition even with the additional usage of authentication and parity bits. The main weakness lies within the technique of using block average intensity. It is crucial that in the tamper localization process in image watermarking to achieve 100% success rate so that any malicious tampering can be detected especially in protecting the medical image.

1.2 PROBLEM STATEMENT

To localise tamper in a block, the watermark need to be embedded directly into that block. If a block is being tampered locally, the intensities of the pixels involved will be changed. This will also change the average intensity of the block concerned. So, in order to ensure that this is not changed, a parity check will be used. However, a parity check is ineffective if more than one bit is changed and causes some tampered area undetected. Besides that, the parity check alone will not guarantee that the block has not been changed, because local tampering usually causes burst error when the same location was tempered with different pixels values. This is because if more than one parity has been changed a parity check is not longer to useful.

1.3 OBJECTIVE

i) To improve tamper localization rate using enhanced block average intensity.

ii) To test medical image watermarking scheme using chosen modality

1.4 SCOPE OF PROJECT

The project scope is help to develop medical image watermarking scheme using enhanced block intensity in order to test the medical image watermarking scheme using chosen modality. The block average intensity can be used to detect the block that has been tampered but cannot be tampered by using the previous method. So, the block average intensity is been enhanced to overcome this problem. The average intensity will significantly reduce the watermark payload because the authentication information is generated for a group of pixels rather than each pixel in an image.

1.5 THESIS ORGANIZATION

This thesis consists of five chapters and each chapter will discuss the different main issues. Below are the summary content for each chapter.

Chapter 1 Introduction

This chapter discuss about the introduction information of the project that includes objectives, scope and problem statement.

Chapter 2 Literature Review

This chapter will presented about the literature review and research paper which related to this research project.

Chapter 3 Methodology

Data analysis and methodology of the project will be discussed more details in this chapter.

Chapter 4 Design

The design of the project development will be described in this chapter.

Chapter 5 Implementation

This chapter will be discussed about the implementation of the project.

Chapter 6 Result and Discussion

The result of the project will be discussed in this chapter.

Chapter 7 Conclusion

This chapter will make a complete summary for the project.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

The literature review of this project will be presented about the technique and equipment that are going to be used in this project.

2.2 TYPE OF DOMAIN

There are many watermarking schemes were proposed for medical images. Those the techniques can be spatial domain technique, frequency domain techniques, or a combination of the two domains.

2.2.1 SPATIAL DOMAIN

Spatial domain is one of the most direct simple techniques in the way to embed the watermark information into the LSBs of the image. The change of gray value is changes according to the change in the LSB, so the modification is not been seen or realize by human eyes. This technique can saying that it is seldom be used.

2.2.2 FREQUENCY DOMAIN

Most of the transform domain techniques embed the watermark information into the transform coefficients of the cover image . The transform domain techniques produces spectral domains where watermarking can be applied. 3 most popular techniques in this category are Discrete Cosine Transform (DCT), Discrete Wavelet Transform(DWT) and Discrete Fourier Transform(DFT) . To overcome the compression and more robust against geometric transformation such as rotation, scaling, translation and cropping the techniques used need have some amount of computation(Song et al.,2010).

2.3 REVERSIBLE WATERMARK

A minor modification to the original content will be performed in the process of watermarking. By introduce some amount of the distortion onto the image the minor modification is needed so that there is enough for the watermarking. In order to maintain the image does not be changed the amount of distortion must be minimize. On the other hand, minor distortion introduced may be acceptable if the watermarked image is depending. Some application such as digital images for military investigate and recognition cannot be acceptable (Fridrich et al., 2002) . The watermarking scheme used on a medical image should be reversible (Coatrieux et al.,2006) .

2.4 REGION OF INTEREST (ROI)

Region of interests is an area of the image can considered as important to the user. The ROI is the significant part of the image which is used for doctor diagnosis purposes in medical image field (Watakani, 2002) . Since the information in medical images is not be modified in anyway the watermark is usually being embedded in the

region of non-interest (RONI) (Liew et al., 2010) . The ROI and RONI were defined before the process of watermark embedding that had been used by (Lim et al.,2008) and (Fotopoulus et al., 2008) .

However, the ability the detection tampering of a watermarking image is a crucial for authentications is allowed. Tampered part can be recovered, once tampering is detected(Wu et al.,2008) and (Jasni et al.,2004). The medical image is be divided into blocks and each block is embedded with the message of authentication and information recovery for other blocks.

Recovery and reversible tamper detection design for the medical images is been proposed by (Liew and Jasni, 2010) . The medical image will be designed using the ROI, RONI and blocks to divide the medical image. In detect the tempering and recovery the authentication bit, parity bit and pixels average intensity will be used.

2.5 MEDICAL IMAGE WATERMARKING

There are 3 types of watermarking methods for medical images had identified by (Coatrieux and Lecornu , 2000) . The first solution is by embeds the watermarking within the RONI so it does not affect clinical diagnosis. The ROI is used for diagnosis rather than RONI which is generally in black. The RONI sometimes can involve gray-level portion of little interest (Shin and Wu, 2005). Since the watermark embedding in the RONI causes no interference with the ROI, invisibility is less strict. However, distortions caused by the watermark embedding in the RONI may annoy physicians. Therefore, the level of distortion has to be kept low. The second method is the reversible watermarking. The watermark is embedded in the image but can be removed so that the image can be restored to its original state. However, this method more often has an issue with low storage capacity when being compared to non-reversible method. The last method focuses on minimizing the distortion caused by watermarking. The watermark replaces some image details such as LSBs of the image or details lost after lossy image compression.

2.6 TAMPER LOCALIZATION

The ability to identify the manipulated area or localization where authentication watermark should be able to detect the manipulated areas location and other areas as authentic location is one of the requirements of an effective watermark based authentication (Liu and Qiu, 2002).

One of the requirements of an effective watermarking based authentication system as defined by (Liu and Qiu, 2002) is the ability to identify manipulated area or also known as localization where authentication watermark should be able to detect the location of manipulated areas and verify other areas as authentic. Some examples of tamper localization watermarking scheme for medical images are as shown below:

2.6.1 OVERVIEW OF WATERMARKING TECHNIQUES

Watermarking schemes can be classified into three categories depending on the purpose:

A. Authentication by using average block intensity schemes

The original image can be recovered completely by using the LSB scheme (Osamah and Khoo, 2011). An SHA-256 hash code is calculated in the embedding processing selected the ROI. Then the hash code will be embedded into LSBs of RONI. The watermark is extracted from LSBs of RONI and those pixels which carried the watermark are set back to 0 at the end of the receiver. Therefore, the original image can be produce before embedding watermark. However, hash values of the extracted image with the extracted hash value are comparing by obtained the authentication. The image is authentic if the hash value is same. For non-zero values, the scheme is not reversible and the reversible

scheme is based on the original values of RONI pixels were zero before embedding.

The improve security of medical images that involve the ability to detect tamper and subsequently recover the image is one of the spatial domain technique (Zain et al., 2006). In this technique, the algorithms of the secret key and a public chaotic are combined together with the simple operations such as parity check and compression to embed to recover a tampered image. However, the image is divided into blocks of 8X8 pixels each in the embedding process (Osamah and Khoo, 2009). Then each block is further divide it into four sub-blocks of 4X4 pixels. The watermark is embedded using LSB's in each sub-block that consists of 3-tuple (v, p, r) where both v and p are 1-bit authentication watermark and r is a 7-bit recovery watermark for corresponding sub-block within one block and map to other block by using mapping function. The v and p are used for tamper detection and localization during the extraction. This scheme is dividing into ROI and RONI into smaller blocks (Zain et al., 2009). Besides that, the 7-bits recovery information are embedded into the corresponding sub-blocks of RONI while the authentication bit, v and p is embedded into ROI sub-blocks. The image quality can be improved by only change of maximum 2 bits in every 4 pixels.

By using the scheme based on modulo 256 and discrete cosine(DCT), first is by divide the image into several blocks, and each block will combined with modulo operation to hide the watermark. The first scheme is embedded each block with the watermark which is a combination of an authentication message and the recovery block is too small and excessively compressed, the second scheme is introduced concept of ROI. The watermark is embedded into RONI only and the combination of bits ROI with the hash value needed in order to form watermark. The original image can be obtained with only the steno image if there is no tamper block. So, an approximate image will be obtained from other blocks when the ROI is been tampered. Only authentication and recovery data are

embedded in the drawback scheme due to limited hiding capacity. Besides that, in order to prevent pixel flipping the scheme cannot be reversible.

B. Authentication and Data-Hiding Schemes

This is the multipurpose scheme as they can achieve various tasks such as hiding patient's report, authenticating the image, localizing the tampered area and recovering those tampered areas when needed.

The frequency domain technique based on discrete wavelet transform (DWT) combined with a quantization method (Giakoumaki et al.,2006). To increase its robustness and security this technique should be gradually improved (Giakoumaki et al.,2006). Based on these technique Haar wavelet coefficients is form and the decreased eye sensitivity to noise in high resolution bands. The physician's digital signature for source authentication and a caption watermark including the patient's personal data, health history and diagnosis reports scheme embeds a robust watermark containing more clear details. Additionally, the image might have been tampered with can be defined by the fragile watermark together with the information. In order to detect the tamper, the fragile watermark can be a reference watermark that used for tamper detection. The drawback of this scheme is the lack of recovery capability in case of tamper detected.

2.6.2 OTHERS EXAMPLES OF SCHEMES

By the way to allow the watermark can be reversible tamper localization watermarking scheme is using the pixel value by modification proposed by (Tan et al., 2011). The Cyclic Redundancy Code (CRC) is calculated for each block and the image is divided into 16X16 pixel blocks. In the event CRC cannot be embedded into its own block so the remaining bits will be carried over to the next blocks. The CRC values are comparing during the comparison indicates tampering and the tampering localization

accuracy is within 16 X 16 pixels. The watermark image can be verified by extracting the watermark. However, there have a disadvantages because if want to allow reversibility, during the embedding process all the pixel value needs to be increased by 4 pixels values to prevent the bit flow out and make the maximum pixel value that allow in an image to be watermarked been constrained.

Besides that, other type of tampering localization techniques is by using average block intensity and divides the image into blocks (Chiang et al., 2008). By taking the average pixel value for each block and embedded as watermark to generate the authentication information. This will allow the retrieved average pixel value from the watermark compare with the current average pixel value of the image and allow the whole image can be confirmed. Tampered region can be localized to accuracy of 4X4 pixels and any mismatch is indicates tampering. The advantage of this scheme is that the watermarking process can be modified to defined ROI rather than to the whole image. The exact pixel value is used to store the recovery information of ROI rather than average pixel values.

Furthermore, (Osama and khoo, 2011) had also proposed the same technique. The image is divided into 16X16 pixel blocks and the ROI is defined. The average intensity of each block is embedded as part of the watermark. However, the average intensity of each block in the ROI is compare with the retrieved average intensity from the watermark in tamper localization. Besides, second watermark is compressed and embedded into RONI by using a DWT technique (transform domain) (Osama and khoo, 2011).

Based on the earlier research tamper localization and recovery watermarking had also been produced (Jasni and Abdul, 2006). The uses block is also a based technique where each block consists of 8X8 pixels. Each block is then further divided into 4X4 pixels of sub-blocks. A three tuple watermark embedded consists of a seven bit recovery watermark for other sub-block and a two-bit authentication watermark. In order to generate the authentication watermark, average intensity of each sub-block is calculated. In a mapping sequence, average intensity of a sub-block is embedded as the seven bit